SPECIFICATION

TITLE

"METHOD FOR THE DEPENDABLE TRANSMISSION OF SERVICE DATA TO A TERMINAL EQUIPMENT AND ARRANGEMENT FOR IMPLEMENTING THE METHOD"

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention is directed to a method, and an arrangement for implementing the method, for dependable transmission of service data to terminal equipment from a remote location, and in particular to a method and arrangement for transmitting and storing a new postage fee table in a postage computer in a secure manner.

Description of the Prior Art

German PS 38 23 719 and United States Patent No. 4,138,735 disclose initiating a reloading of a fee schedule table for postage fees from a remote data central at specific points in time. If the data exchange is initiated by the server of the data center, the postage meter machine must remain constantly activated, which is, of course, disadvantageous.

Alternatively, United States Patent Nos. 5,490,077 and United States Patent No. 5,606,508 disclose initiating the data loading on demand by the postage meter machine, with the data base being updated dependent on conditions (such as, for example, name, date) after the postage meter machine is turned on. In order to be able to equip a large number of postal customers with a fee schedule table in the relatively short time between the promulgation and the effective date of a new fee schedule, the new fee schedule is stored in a memory of a transmission means (chip card or cell of

a GSM network) separated from the postage meter machine far before it takes effect. When the postage meter machine is turned on, the date of the calender module of the postage meter machine is employed or is combined with further input conditions in order to select the table that is loaded into the memory thereof when the postage meter machine is initialized. An updating of the previous table ensues by downloading the memory of the transmission means into of the memory of the postage meter machine.

United States Patent No. 5,710,706 (corresponding to European Application 724 141) discloses a data input into a scale that is connected by an interface to a postage meter machine in order to update fee schedule table data with new data. The loading of the new data ensues by modem to the postage meter machine from a remote data center. The loading and updating ensue in immediate succession. When fee schedule table data are to be updated, a loading ensues and, given intermediate storage of fee schedule table data in the postage meter machine, a sector-by-sector deletion of the old postage table ensues in the non-volatile memory of the scale before the transmission of the new fee schedule table data from the intermediate memory of the postage meter machine to the scale and the write-in of the new fee schedule table data in the non-volatile memory of the scale. A number of tables can be stored in the scale, however, each table relates to a separate mail carrier that can be selected via a keyboard. The minimum validity of a fee schedule table allocated to a carrier identification number CIN is stored and interpreted by the postage meter machine in order, when needed, to form request data for loading new fee schedule table data, or for updating in the memory of the scale according to the CIN.

United States Patent No. 5,448,641 discloses a postal fee system wherein a validity check is made in the terminal equipment at the user side. The postage fee schedule table is transmitted from the data center to the terminal equipment. A code belonging to the postage fee schedule is also transmitted from the data center to the terminal equipment. The latter generates a comparison code from information based on the received postage fee schedule table. On the basis of the comparison of the received code to the generated comparison code, the validity of the received postage fee schedule table can be checked in the terminal equipment. Although the terminal equipment can verify the communicated postage fee schedule table, the data center cannot check whether the current postage fee schedule table was in fact properly stored by the terminal equipment. In case of disagreement, the user could delay payment of the service or refuse it because no documentation exists about the storage of the postage fee schedule table that ensued in the terminal equipment. The manufacturer of the postage meter machine thus count not avoid an on site inspection of the machine.

SUMMARY OF THE INVENTION

An object of the present invention is to provide an arrangement and a method for the dependable transmission of service data to a terminal equipment which allows for proper storage of service data to be checked, particularly a communicated postage fee schedule table, which avoids the aforementioned shortcomings of the prior art. The check should ensue automatically, preferably without input on the part of the user of the terminal equipment. The terminal equipment should not be blocked (unavailable for use) for an unnecessarily long time.

The invention responds to the need of some mail carriers to freely modify service data, particularly the fees in postage fee schedule tables. The service data are required to be stored in a processing module at the terminal equipment.

The processing module is an electronic postage computer. The terminal equipment is connected to a postage computer, or the terminal equipment can contain a microprocessor serving as a postage computer, the postage computer being programmed to undertake a storage of the new postage fee schedule table data in a memory of the terminal equipment or of the postage computer, and to form a checksum over the stored, new postage fee schedule table data and to communicate the checksum to the data central, as well as to implement a received (OK) message and switch the terminal equipment or the postage computer into an operating mode.

Alternatively, the microprocessor of the terminal equipment or of the postage computer can be programmed to undertake an intermediate storage of the new postage fee schedule table data in volatile main memory of the terminal equipment or of the postage computer, and to form a checksum over the intermediately stored, new postage fee schedule table data and communicate the checksum to the data center, as well as to implement a load instruction of the data center at the terminal equipment upon reception of an OK message, so as to load the new postage fee schedule table data into a non-volatile memory of the postage computer and to subsequently switch the terminal equipment or the postage computer into an operating mode.

When service data are required, particularly a modified postage fee schedule table in an electronic postage computer, accordingly, a remote loading procedure can ensue. Carriers (governmental or commercial) respectively commission (approve) a

data center to offer the service of remote loading, i.e., to communicate service data to the terminal equipment on demand in order to be able to load the service data into corresponding memories of the terminal equipment's processing module. In such a remote loading procedure, the inventive method for reliable transmission of service data to a terminal equipment is utilized with the following method steps:

- offering new service data in the data center for a future processing based on the service data;
- forming request data for service data at the terminal equipment;
- conducting a first communication between the terminal equipment and a data center wherein the terminal equipment transmits the request data in order to request the new service data from the data center and wherein the request data are received in the data center and the data center transmits the requested service data to the terminal equipment the received requested data then being intermediately stored at the terminal equipment;
- conducting a second communication between the terminal equipment and the data center, wherein the terminal equipment formulates a message that refers to the content of the intermediately stored, valid, new service data and transmits this message to the data center, and wherein the data center receives and checks the message on the basis of a comparison with information generated from the service data and, wherein the data center transmits a message to the terminal equipment, with a registration

of the service performed ensuing in the data center in conjunction with the transmission of this message.

The communication from the data center can ensue by modem directly with the processing module in the terminal equipment or indirectly with the processing module via the terminal equipment.

The initially volatilely intermediately stored, valid, new service data are processed by the processing module to form a checksum. A message is then formed and is communicated from the terminal equipment to the data center. The message communicated to the data center preferably contains an identification of the terminal equipment (for example, a PIN), a version number and the checksum over the service data or an encrypted checksum, or a signature. The new service data (intermediately) stored in the processing module or terminal equipment thus can be identified in the data center and their proper or error-free (intermediate) storage can be verified. The terminating message sent by the data center is, for example, a load instruction to load the new surface data into a non-volatile memory of a processing module.

The postage computer can be integrated in the terminal equipment or can be arranged separate from the terminal equipment. The terminal equipment is preferably a postage meter machine, with a symmetrical encryption algorithm for forming an encrypted checksum and a secret key being stored in secure form in the postage meter machine.

Alternatively, the postage computer can be integrated in a scale. In this case an asymmetrical encryption algorithm for forming an encrypted checksum and a public key are stored in the scale, with the public key being stored in an unsecured manner.

DESCRIPTION OF THE DRAWINGS

Figure 1a is a block circuit diagram of a postage meter machine with postage computer constructed and operating in accordance with the invention.

Figure 1b is a block circuit diagram of a version of the postage meter machine of Figure 1a having an OTP.

Figure 1c is a block circuit diagram of a postage meter machine with a postage-calculating scale.

Figure 2 is a flowchart for the dependable transmission of data in accordance with the invention.

Figure 3a is a flowchart for a first embodiment for checking the transmitted data in accordance with the invention.

Figure 3b is a flowchart for a second embodiment for checking the transmitted data in accordance with the invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1a shows a block circuit diagram of the inventive postage meter machine with a printer module 1 for a completely electronically generated franking image. This postage meter machine has at least one input unit 2 with a number of actuation elements, a display unit 3, a modem 23 that produces the communication with a data center. A further input unit 21 and/or a scale 22 is/are coupled to a control unit 6 via an input/output control module 4. The postage meter machine has non-volatile memories 5a, 5b, 9, 10 and 11 for data that contain the variable or the constant parts of the franking image and programs for processing the data in conjunction with the mail carrier and service to be carried out by the carrier (as explained below).

Further explanations about individual functions of the aforementioned components are provided in German OS 19534530, corresponding to United States Patent No. 5,805,711. A character memory 9 supplies the necessary print data for the variable parts of the franking image to a volatile main memory 7. The control unit 6 is a microprocessor μP that is in communication with the input/output control module 4, the character memory 9, the volatile main memory 7 and non-volatile main memories 5a, 5b containing internal, non-volatile fee schedule memories. Alternatively, (shown in broken lines) an additional, non-volatile fee schedule memory 16 can be used. The control unit 6 is also in communication with a non-volatile advertising slogan/graphics memory 10 and program memory 11, with the motor of a transport or feeder means, possibly with a tape dispenser 12, an encoder (coding disk) 13, as well as a clock/date module 8. That memory module that includes the non-volatile main memory 5b can, for example, be an EEPROM that is protected against removal by at least one additional measure, for example gluing on the printed circuit board, sealing or casting with epoxy resin. The storage of the postage fee schedule tables can be realized separately or, for example, within the non-volatile memory 5a by providing special memory areas. The individual memories can be realized as a number of physically separated modules or can be combined in a few modules. A fee schedule table which will become valid in the future is stored in the memory area 16-01 provided therefor and the current valid fee schedule table is stored in the separately provided memory area 16-02. The available memory capacity in the non-volatile memory amounts, for example, to 20 kBytes and is optimally utilized on the basis of space-saving memory space management. The non-volatile fee schedule memory is preferably a battery supported CMOS-RAM module. In a preferred version of the embodiment, it includes a third

memory area 16-03 in which the checksum formed for the respectively desired postage fee schedule table is stored allocated to a version number.

Obtaining the postage fee schedule table data from the data center ensues as needed or in conjunction with the remote loading of the postage meter machine with a credit (postage call for the purpose of re-crediting), with the security measures of the credit loading being utilized also for the table loading. The postage fee schedule table data are initially intermediately stored in the memory area 70 of the volatile main memory RAM 7 of the postage meter machine. The microprocessor 6 can now form a checksum over the content of the postage fee schedule table data and send this checksum by modem 23 to the data center DZ land-line or radio via a communication network. The data center DZ has a modem 33 that is connected to a server 32 that accesses a data bank 31. The requesting postage meter machine identifies itself at the data center with its PIN (postage call identification number) and communicates the version number for the purpose of locating a new postage fee schedule table in the data bank DB31 of the data center, wherein a postage fee schedule table is allocated to the communicated version number. The server 32 is programmed for checking the proper transmission and error-free intermediate storage of service data on the basis of the checksum, as will be explained in yet greater detail with reference to Figures 3a and 3b.

Details of the block circuit diagram of the electronic postage meter machine for a version with an OTP (one time programmable) processor as the control unit 6 are shown in Figure 1b, as disclosed in the aforementioned German OS 19534530, as well as in German Patent Application 19731304.3-53, corresponding to United States Application Serial No. 09/115,048 filed July 14, 1998. The CPU 6a forms the checksum

on the basis of the communicated table that has been volatilely intermediately stored. The intermediate storage of the communicated table can, for example, also ensue in the internal main memory iRAM 6b instead of in the volatile main memory RAM 7 or using both main memories.

Figure 1c shows a block circuit diagram of the electronic postage meter machine for a version with a postage-calculating scale. The fee schedule memory 16 and the postage computer are components of the postage-calculating scale 22a here. The latter utilizes the modem 23 of the postage meter machine for communication with the data center DZ.

When a modified postage fee schedule table is required in an electronic postage computer, a remote installation can ensue on demand. A postage fee schedule table is to be communicated to the terminal equipment on demand in order to be able to load this into corresponding memories of the postage computer. Given such a remote installation, one embodiment of the inventive method for dependable transmission of service data to a terminal equipment proceeds according to the following method steps:

In step 210, new postage fee schedule table data are offered in the data center for a future postage calculation. In step 110 the terminal equipment (postage calculator) formulates request data for postage fee schedule table data. In a first communication 120 of the terminal equipment with the data center, the request data are transmitted in order to request the new postage fee schedule table data from the data center, and comprising a reception and storing of the requested postage fee schedule table data are subsequently received and stored by the terminal equipment. In a first communication 220 of the data center with the terminal equipment, the aforementioned

request data are received at the data center and the requested postage fee schedule table data are transmitted to the terminal equipment. In a second communication 130 of the terminal equipment with the data center, a message is formed at the terminal equipment and is communicated to the data center, that refers to the stored, valid, new postage fee schedule table data. In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and an OK message is transmitted to the terminal equipment, and in step 240 a registration of the service performed ensues in the data center in conjunction with the transmission of an OK message.

Upon reception of the OK message in the terminal equipment, an indicator that the stored data is registered in valid form ensues and a flag for payment of the service ensues in the data center. As the indicator, either a bit is set in a secured area in the non-volatile memory of the postage computer or corresponding MAC-protected data are stored. The microprocessor only utilizes data registered as valid for calculating postage.

The following method steps proceed in an alternative embodiment:

In step 210, new postage fee schedule table data are offered in the data center for a future postage calculation. In step 110 the terminal equipment (postage calculator) formulates request data for postage fee schedule table data. In a first communication 120 of the terminal equipment with the data center, the request data are transmitted in order to request the new postage fee schedule table data from the data center, and comprising a reception and storing of the requested postage fee schedule

table data are subsequently received and stored by the terminal equipment. In a first communication 220 of the data center with the terminal equipment, the aforementioned request data re received at the data center and the requested postage fee schedule table data are transmitted to the terminal equipment. In a second communication 130 of the terminal equipment with the data center, a message is formed at the terminal equipment and is communicated to the data center, that refers to the stored, valid, new postage fee schedule table data. In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and an OK message is transmitted to the terminal equipment, and in step 240 a registration of the service performed ensues in the data center in conjunction with the transmission of an OK message.

In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and a load instruction is transmitted to the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of its postage computer.

A registration (step 240) of the loading ensues in the data center, and loading (step 140) of the postage fee schedule table data into a non-volatile memory of the postage computer ensues after reception of the load instruction.

Advantageously, the communication from the data center can ensue by modem directly with the postage meter machine or postage-calculating scale or can ensue

indirectly to the postage-calculating scale via the postage meter machine, as disclosed in United States Patent Nos. 5,606,508 and 5,710,706.

According to United States Patent No. 5,606,508, the postage computer is arranged inside the electronic postage meter machine and a scale is connected to the electronic postage meter machine only for communicating weight. Alternatively, as disclosed in United States Patent No. 5,710,706, a postage-calculating scale is equipped with an electronic postage computer. The postage value thus already can be determined by the postage-calculating scale on the basis of the measured weight and can be supplied as an input to the postage meter machine. In these known arrangements, a non-volatile intermediate storage of the postage fee schedule table occurs, for example in a chip card or in the memory of a GSM network, the data tables being taken therefrom for loading.

Differing therefrom, a volatile intermediate storage of the communicated table in a volatile main memory of the terminal equipment or of the postage computer is initially adequate in the alternative embodiment of the inventive method. The terminal equipment is connected to a postage computer in which storage of the new postage fee schedule table data ensues.

The postage computer can be integrated in the terminal equipment or can be arranged separated from the terminal equipment. The intermediate storage ensues in the volatile main memory RAM 7 in order to form a checksum with the control unit (microprocessor) 6. The postage computer forms the checksum over the content of the table according to a known algorithm that is stored in the program memory 11. The information communicated to the data center preferably contains the version number

and a checksum over the postage fee schedule table data in a predetermined mathematical operation, or contains an encrypted checksum, or a signature. Known symmetrical or asymmetrical algorithms are utilized for encryption.

In a second version of the arrangement an OTP processor is used which allows the formation of a DES-encrypted checksum, whereby the symmetrical DES (data encryption standard) algorithm and the secret DES key are stored in a secure manner in the postage meter machine. Alternatively, a checksum can be communicated from the separate postage computer to the postage meter machine, which has a secure housing with special measures to protect against tampering. The postage meter machine then forms a DES-encrypted checksum, with the DES key required for this purpose being stored in a secure manner in the postage meter machine in a known way.

In an other version the postage computer is integrated in a scale or is arranged separated from the terminal equipment. The postage computer contains a program memory having an asymmetrical encryption algorithm and having a public key. The latter, which need not be particularly protected in the manner of a secret key, can consequently likewise be non-volatilely stored in a memory of the scale.

The RSA algorithm (named for its inventors R. Rivest, A. Shamir, L. Adleman) is a suitable known asymmetrical encryption algorithm. This is advantageous when no secured housing is available for the protection of the keys. For example, an RSA-encrypted checksum is formed in the scale, with an RSA key being employed that is stored in the scale as a public key and thus such storage need not be secured.

Figure 2 shows a flowchart for the dependable transmission of data to the terminal equipment in according with the inventive method. The data center starts in step 200 and offers new postage fee schedule tables in the following step 210. For example, the terminal equipment is a postage meter machine that is started when turned on (step 100). The postage meter machine contains a postage computer that, in step 110, forms request data for new postage fee schedule table data. In one version of the method an automatic unit forms request data in order to be able to access current tables when the point in time for new postage fee schedule table data comes close. This automatic unit works dependent on the carrier that has been set and on the date supplied to the postage meter machine by the clock/date module 8. The automatic unit can be realized in the postage computer and/or in the memory cells of the clock/date module 8. Alternatively, the postage computer can be integrated in a postage-calculating scale 22a that is connected by interface to the postage meter machine.

The communication between the terminal equipment, i.e. the postage meter machine, and the data center proceeds in two transactions. The first transaction 120 begins with a transmission of the request data in order to request the new postage fee schedule table data from the data center and ends with reception and intermediate storage of the requested postage fee schedule table data in a volatile main memory RAM 7d. Proceeding in parallel at the data center is a communication (step 220) of the data center with the terminal equipment, including a reception of the request data in the data center and transmission of the requested postage fee schedule table data to the terminal equipment, i.e. to the postage meter machine.

The second transaction 130 at the terminal equipment begins with formation of a message in the terminal equipment, i.e. in the postage meter machine, this message referring to the intermediately stored, valid, new postage fee schedule table data. The communication of the terminal equipment with a data center is continued with the communication of the message from the terminal equipment to the data center and reception of the OK message, and/or a load instruction. Proceeding in parallel at the data center is a second communication (step 230) of the data center with the terminal equipment, including reception and checking of the information in the data center on the basis of a comparison with information generated from the postage fee schedule table data, and transmission of an OK message and/or a load instruction to the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of the postage computer. In step 140, the received OK message is implemented; loading of a new postage fee schedule table data ensues when a valid load instruction is received. Otherwise, the second communication is repeated if no OK message was received.

In parallel therewith, a registration (step 240) of the service in a data bank of the data center is undertaken at the data center for the purpose of billing and accounting or later payment. A branch is then made back to step 210.

In the preferred example with the postage computer in the electronic postage meter machine, the postage meter machine - in addition to sending its PIN - sends a version number and the checksum to the data center, making it possible for the data center to unambiguously identify the transmitted, new fee schedule table data. Before the fee schedule table data stored intermediately in the postage meter machine are

recognized as valid, a check of the checksum is also implemented in the data center. The aforementioned message preferably contains the version number of the table and an encrypted checksum in order to enable a verification of the properly communicated and intermediately stored table. An encrypted checksum can be employed as a digital signature that refers to the volatilely intermediately stored, valid, new postage fee schedule table data, however, further data can enter into the message or can be encrypted therewith.

Figures 3a and 3b show first and second versions of a flowchart for checking the dependable transmission of data to the terminal equipment.

In one version, shown in Figure 3a, the encrypted checksum is formed by the postage computer on the basis of an asymmetrical encryption algorithm, a public key being stored therein, and an appertaining, private, secret key (PRIVATE KEY) is employed for checking in the data center, this being stored in a secure manner and being kept secret from third parties. Given an RSA signature, a message based on the version number and on the checksum is encrypted with a public write key (PUBLIC KEY) to form a digital signature. The digital signature (SIGNATURE) is sent from the terminal equipment to the data center together with the identification number PIN and the version number (VERSION NO), the data center being capable of decrypting the signature with a secret read key (PRIVATE KEY) according to the asymmetrical algorithm (RSA). The checksum (CHECK SUM) over the content of the fee schedule table data that are stored in the data bank 31 allocated to the version number (and possibly also allocated to the PIN) must agree with the decrypted message if the fee schedule table data intermediately stored in the postage computer or in the postage

meter machine are to be recognized as being valid. This verification is a prerequisite in order to communicate a corresponding command to the postage meter machine. The rate table check sum formation can ensue before or during the communication. A prior formation has the advantage that the comparison check sum RATE TABLE CHECK SUM is stored in the data bank 31 allocated to the version number VERSION NO. or PIN and can be called directly from the data bank 31 by the server 32 for comparison. The calculating time of the server 32 that is saved is thus advantageously available to the decryption procedure of the SIGNATURE. The decrypted message is identical to the checksum CHECK SUM that was formed in the postage computer or terminal equipment from the volatilely intermediately stored postage fee schedule table. Given proper intermediate storage, the decrypted checksum CHECK SUM is identical to the comparison checksum RATE TABLE CHECK SUM that is formed or stored in the data bank 31.

The digital signature algorithm (DSA) according to United States Patent No. 5,231,668 is also known for producing the RSA signature. Fundamentally, however, any other arbitrary asymmetrical algorithm can be utilized, for example the ELGamal algorithm (ELGA) or the elliptic curve signature scheme (ECSS).

In another version, shown in Figure 3b, an encrypted checksum MAC (message authentication code) is formed with a symmetrical encryption algorithm, this being formed by the postage meter machine in which a secret key is stored. The encrypted checksum MAC is communicated to the data center. Differing from the version shown in Figure 3a, no decryption is implemented in the data center; rather, an encryption is implemented in order to encrypt a checksum derived from the postage fee schedule

table to form a comparison MAC'. The RATE TABLE CHECK SUM formation can ensue before or during the communication. Such a prior formation has the advantage that the CHECK SUM merely has to be called from the data bank 31 in order to generate the comparison MAC' from this CHECK SUM by encryption with a secret key SECRET KEY using a symmetrical algorithm DES with the assistance of the server 32.

The same secret key SECRET KEY is employed in the check in the data center as in the postage meter machine. The check in the data center preferably ensues with both MACs. A suitable version of the DES algorithm is preferably utilized in the MAC formation. The same secret DES key is employed given a MAC formation in the data center and in the postage meter machine. To that end, the secret DES key must be stored secured in the data bank 31 allocated to that PIN identifying the terminal equipment. Alternatively, the RATE TABLE CHECK SUM formation and the encryption to form a comparison MAC can ensue in common before the communication. The comparison MAC is then stored in the data bank 31 allocated to the PIN and to the version number and can be called by the server for comparison purposes.

Newer postage meter machines utilize digitally operating printing units. For example, the postage meter machines T1000 and JetMail of Francotyp-Postalia AG & Co. are the first to exhibit a thermo transfer printer and an ink jet printer, respectively. It is thus fundamentally possible to print different information or to arbitrary print in some other way on a filled envelope in the region of the franking stamp, this other information having a corresponding relationship to a service of a carrier. It is thus easily possible to change between private mail carriers and their services. The franking stamp imprint

therefore advantageously contains a reference to the carrier and/or the service being used.

Although modifications and changes may be suggested by those skilled in the art, it is the intention of the inventor to embody within the patent warranted hereon all changes and modifications as reasonably and properly come within the scope of his contribution to the art.